DaimlerChrysler AG

Patent claims

1. A method for loading at least one current application program (flashware) which is stored in a program memory (flash) of a microprocessor system (ECU), in which method the following are connected to the processor bus (PBUS) of the microprocessor system (ECU)

- at least one microprocessor (CPU),
- at least one program memory with a boot sector, a flash boot loader, an electrically erasable and programmable memory (flash) and a read-write memory (RAM),
- and at least one system interface (diagnostic interface, onboard power system interface),

and in which method

- an authentication code (HMAC) is produced for the application program (flashware),
- the authentication code (HMAC) and the current application program are read in via the system interface,
- and, before the read-in current application program is actuated, the authentication code (HMAC) which has been read in at the system interface is checked, characterized in that the authentication code (HMAC) is calculated in a secured area (trust center) by concatenating the application program (flashware) with a secret data string (STRING) and calculating a hash value from the concatenated application program, which hash value is read in as an authentication code (HMAC) at the system interface, and in that a second, identical, secret data string (STRING) with which the read-in application program (flashware) is concatenated in the microprocessor system is stored in the microprocessor system, and a hash value is calculated by the read-in, concatenated application program in the microprocessor (CPU) and is compared with the

transmitted authentication code (HMAC).

2. The method as claimed in claim 1, characterized in that the application program is concatenated with the secret data string in the microprocessor at the start of the program and at the end of the program both in the secured area (trust center) and during the authenticity checking, and a hash value is calculated by the application program which is concatenated at both ends and said hash value is read in as an authentication code (HMAC) at the system interface.

3. The method as claimed in claim 1, characterized

- in that the application program is initially concatenated with the secret data string (STRING) either at the start of the program or at the end of the program,
- in that, in a following step, a first hash value (HMAC1) is calculated in the secured area (trust center) by the application program which is concatenated at one end,
- in that, in a further following step, the first hash value (HMAC1) is concatenated with a secret data string (STRING) at one end,
- in that, in a further following step, a second hash value (HMAC) is calculated by the combination of a first hash value (HMAC1) and secret data string (STRING), and said second hash value (HMAC) is read in as an authentication code (HMAC) at the system interface,
- and in that a second, identical, secret data string (STRING) is stored in the microprocessor system and the steps carried out in the secured area (trust center) are repeated with the original application program in the same sequence using said data string (STRING) in the microprocessor,
- and the hash value which is calculated in the microprocessor are compared with the hash value (HMAC) which is read in at the system interface.

4. The method as claimed in one of claims 1 to 3, characterized in that the authentication code (HMAC) is transferred together with the application program (flashware).

5. The method as claimed in one of claims 1 to 3, characterized in that the authentication code (HMAC) is transferred separately from the application program (flashware).

6. The method as claimed in claim 5, characterized in that the application program (flashware) is buffered on a memory medium and marketed by means of the memory medium, and the authentication code (HMAC) is transmitted to the system interface from the secured area (trust center) by means of data transmission.

7. The method as claimed in claim 4, characterized in that the application program (flashware) and the authentication code (HMAC) are transmitted to the system interface from the secured area (trust center) by means of data transmission.

8. The method as claimed in one of claims 1 to 7, characterized in that the authentication code is read into a control unit (ECU) of a motor vehicle via the diagnostic interface.

9. The method as claimed in one of claims 1 to 8, characterized in that if a read-in authentication code (HMAC) and a hash value calculated in the microprocessor correspond, the associated application program (flashware) is provided with an identifier (flag) as a valid application program.

10. The method as claimed in one of claims 1 to 9, characterized in that flashware meta information is included in the authentication code (HMAC).

11. The method as claimed in claim 10, characterized in that the authentication code (HMAC) is used to select the download process of the application program on various control units.

12. A method for safeguarding the authenticity of the flashware for a control unit (ECU) of a motor vehicle in which an application program is stored in a program memory (flash), characterized in that an authentication code (HMAC) in which the application program (flashware) is concatenated with a secret data string (STRING) is calculated in a secured area (trust center), and a hash value is calculated by the concatenated application program and is read in as an authentication code (HMAC) into the control unit (ECU), and in that a second, identical, secret data string (STRING) with which the read-in application program (flashware) is concatenated in the control unit is stored in the control unit (ECU), and a hash value is calculated by the read-in, concatenated application program in the control unit (ECU) and is compared with the transmitted authentication code (HMAC).

13. The method as claimed in claim 12, characterized in that the application program is concatenated with the secret data string in the control unit (ECU) at the start of the program and at the end of the program both in the secured area (trust center) and during the authentication checking, and a hash value is calculated by the application program which is concatenated at both ends and said hash value is read in as an authentication code (HMAC) at the system interface.

14. The method as claimed in claim 12, characterized

- in that the application program is initially concatenated with the secret data string (STRING) either at the start of the program or at the end of the program,

- in that, in a following step, a first hash value (HMAC1) is calculated in the secured area (trust center) by the application program which is concatenated at one end,
- in that, in a further following step, the first hash value (HMAC1) is concatenated with a secret data string (STRING) at one end,
- in that, in a further following step, a second hash value (HMAC) is calculated by the combination of a first hash value (HMAC1) and secret data string (STRING), and said second hash value (HMAC) is read in as an authentication code (HMAC) at the system interface,
- and in that a second, identical, secret data string (STRING) is stored in the control unit (ECU) and the steps carried out in the secured area (trust center) are repeated with the original application program in the same sequence using said data string (STRING) in the control unit (ECU),
- and the hash value which is calculated in the control unit (ECU) is compared with the hash value (HMAC) which is read in at the system interface.

15. The method as claimed in one of claims 12 to 14, characterized in that the authentication code (HMAC) is transferred together with the application program (flashware).

16. The method as claimed in one of claims 12 to 14, characterized in that the authentication code (HMAC) is transferred separately from the application program (flashware).

17. The method as claimed in claim 16, characterized in that the application program (flashware) is buffered on a memory medium and marketed by means of the memory medium, and the authentication code (HMAC) is transmitted to the system interface from the secured

area (trust center) by means of data transmission.

18. The method as claimed in claim 15, characterized in that the application program (flashware) and the authentication code (HMAC) are transmitted to the system interface from the secured area (trust center) by means of data transmission.

19. The method as claimed in one of claims 12 to 18, characterized in that the authentication code is read into a control unit (ECU) of a motor vehicle via the diagnostic interface.

20. The method as claimed in one of claims 12 to 19, characterized in that if a read-in authentication code (HMAC) and a hash value calculated in the control unit correspond, the associated application program (flashware) is provided with an identifier (flag) as a valid application program.

21. The method as claimed in one of claims 12 to 20, characterized in that flashware meta information is included in the authentication code (HMAC).

22. The method as claimed in claim 21, characterized in that the authentication code (HMAC) is used to select the download process of the application program on various control units.